Application Number 10/608,767
Amendment in response to Office Action mailed June 13, 2008

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

Claim 1 (Previously Presented) A method comprising:

receiving, with a forensic device coupled to a target computing device via a communication link, input from a remote user of a client device that identifies computer evidence to acquire from the target computing device;

acquiring the computer evidence from the target computing device with the forensic device without pre-loading acquisition software on the target computing device prior to acquiring the computer evidence;

storing the computer evidence on the forensic device; and

presenting a user interface for the forensic device through which the remote user views and analyzes, using the client device, the computer evidence acquired from the target computing device.

Claim 2 (Original) The method of claim 1, wherein presenting the user interface for the forensic device through which the remote user views and analyzes the computer evidence acquired from the target computing device comprises presenting the user interface for the forensic device through which the remote user views and analyzes the computer evidence acquired from the target computing device on-line.

Claim 3 (Original) The method of claim 1, further comprising acquiring additional computer evidence while the remote user views and analyzes the previously acquired computer evidence.

Claim 4 (Original) The method of claim 1, wherein acquiring the computer evidence from the target computing device comprises acquiring the computer evidence from the target computing device while the target computing device is active.

Claim 5 (Original) The method of claim 1, further comprising receiving input from the remote user instructing the forensic device to analyze the computer evidence.

Claim 6 (Previously Presented) The method of claim 1, wherein acquiring the computer evidence from the target computing device comprises acquiring state information from the target computing device that includes at least one of running process information and open network ports with associated processes.

Claim 7 (Cancelled)

Claim 8 (Original) The method of claim 1, wherein receiving input from the remote user that identifies computer evidence to acquire comprises receiving input from the remote user that identifies at least one acquisition operation to perform, and further wherein acquiring the computer evidence from the target computing device comprises performing the acquisition operation to acquire the computer evidence.

Claim 9 (Original) The method of claim 8, wherein performing the acquisition operation comprises communicating commands associated with the acquisition operation to the target computing device to acquire corresponding computer evidence.

Claim 10 (Original) The method of claim 9, further comprising:

automatically selecting at least one of a plurality of access methods via which to perform the acquisition operation based on the target computing device and the type of computer evidence to acquire; and

communicating commands associated with the acquisition operation to the target computing device via the selected acquisition methods.

Claim 11 (Original) The method of claim 10, wherein the access methods include at least one of Windows Management Instrumentation (WMI), Server Message Block (SMB), Secure Shell (SSH), Remote Shell (RSH), Network File System (NFS), Apple Filing Protocol (AFP), File Transfer Protocol (FTP), and Hypertext Transfer Protocol (HTTP).

Claim 12 (Original) The method of claim 8, wherein the remote user identifies a plurality of the acquisition operations to perform, and wherein acquiring the evidence comprises performing the acquisition operations in an order that reduces the impact on other data stored on the target computing device.

Claim 13 (Original) The method of claim 12, further comprising performing a subset of the acquisition operations to acquire at least one of an log file and communication statistics prior to performing the other acquisition operations.

Claim 14 (Original) The method of claim 13, further comprising performing the acquisition operation to acquire the communication statistics after performing the acquisition operation to acquire the log file.

Claim 15 (Original) The method of claim 13, further comprising performing the acquisition operation to acquire the log file after performing the acquisition operation to acquire the communication statistics.

Claim 16 (Original) The method of claim 13, further comprising performing an acquisition operation to acquire general system information from the target computing device after performing the subset of the acquisition operations to acquire the at least one of the log file and communication statistics prior to any other acquisition operations.

Claim 17 (Original) The method of claim 13, wherein the log file comprises one of a system event log, an application event log, and a security event log, web server log file, Unix SYSLOG file, a mail log file, an accounting log file, and a router flow log file.

Claim 18 (Original) The method of claim 13, wherein the communications statistics comprises one of Ethernet statistics and network protocol statistics.

Claim 19 (Original) The method of claim 13, further comprising determining an order in which to perform acquisition operations.

Claim 20 (Original) The method of claim 1, further comprising receiving authentication information from the user to verify the identity of the user.

Claim 21 (Original) The method of claim 20, wherein the authentication information comprises one of a digital certificate or a username and password.

Claim 22 (Original) The method of claim 1, further comprising:

receiving case information and target device information from a user to define a new inquiry;

creating a new inquiry based on the received information; and

associating the new inquiry with a case.

Claim 23 (Original) The method of claim 22, wherein the case information comprises at least one of a case number, case name, principle investigator, location to store the collected data, and a time zone for date/time reporting.

Claim 24 (Original) The method of claim 22, wherein the target computing device information includes at least one of a target computing device host name, IP address, operating system, access methods and password.

Claim 25 (Original) The method of claim 1, further comprising storing a copy of the computer evidence originally acquired from the target computing device.

Claim 26 (Original) The method of claim 1, further comprising:

normalizing the acquired computer evidence to a common format; and

storing the normalized computer evidence.

Claim 27 (Original) The method of claim 26, wherein normalizing the acquired computer evidence to a common format comprises at least one of converting timestamp data from a local time zone of the target computing device to a standard time zone, converting data having host names and IP addresses to all host names, converting data having host names and IP addresses to all IP addresses, and normalizing the clock of the target computing device to that of the forensic device.

Claim 28 (Original) The method of claim 1, further comprising:

performing a cryptographic hash on the computer evidence; and

storing the resulting hash value.

Claim 29 (Original) The method of claim 1, further comprising maintaining an audit log of transactions performed by the forensic device.

Claim 30 (Original) The method of claim 29, wherein maintaining the audit log comprises at least one of tracking computer evidence downloaded from the target computing device, browsing of the computer evidence by the remote user, and analyses performed on the computer evidence, and wherein the audit log comprises a timestamp corresponding to each transaction, an investigator identifier corresponding to the investigator performing each transaction, and a description of each transaction.

Claim 31 (Original) The method of claim 1, wherein the computer evidence comprises at least one log file, the method further comprising:

receiving input from the user to analyze the log file for tampering;

analyzing the log file to detect log file tampering; and

displaying to the user the results of the analysis.

Claim 32 (Original) The method of claim 31, wherein analyzing the log file to detect log file tampering comprises determining whether the entries in the log file are in ascending order.

Claim 33 (Original) The method of claim 31, wherein analyzing the log file to detect log file tampering comprises:

computing time gaps between entries of the log file;

identifying anomalous time gaps; and

displaying to the user the identified anomalous gaps.

Claim 34 (Original) The method of claim 31, wherein analyzing the log file to detect log file tampering comprises:

computing time gaps between entries of the log file;

generating a graphical representation of the time gaps; and

displaying the graphical representation to the user.

Claim 35 (Original) The method of claim 31, wherein analyzing the log file to detect log file tampering comprises:

receiving input that identifies a periodic event;

detecting an absent periodic event within the log file; and

alerting the user of the absent periodic events.

Claim 36 (Original) The method of claim 35, wherein receiving input that identifies the periodic event comprises:

receiving input that identifies a period of the periodic event; and

receiving input that identifies an identifier associated with the periodic event.

Claim 37 (Original) The method of claim 36, wherein detecting absent periodic events within the log file comprises:

searching for the log file for the periodic event identifier;

computing the amount of time that elapsed between each of the periodic event identifiers; and

comparing the period of the event with the computed elapsed times to detect absent periodic events.

Claim 38 (Original) The method of claim 35, wherein identifying the periodic event comprises receiving input from the user identifying the periodic event.

Claim 39 (Original) The method of claim 1, wherein acquiring the computer evidence from the target computing device comprises acquiring an image of at least one of a disk attached to the target computing device and a memory of the target computing device, and further comprising examining the acquired image to identify at least one of files, process or operating system data structures, boot information, deleted files or directories, and data hidden in unallocated space.

Claim 40 (Previously Presented) The method of claim 1, wherein the communication link comprises a customer network of the target computing device.

Claim 41 (Previously Presented) The method of claim 1, wherein the client device is coupled to the forensic device via one of a public network, a customer network of the target computing device, a phone line, a universal serial bus (USB), a wireless port, a serial port, a parallel port and an infrared link.

Claim 42 (Original) The method of claim 1, wherein the target computing device comprises one of a personal computer, a handheld computer, a laptop, a workstation, a router, a gateway device, a firewall device, a web server, a file server, a database server, a mail server, a print server, a network-enabled personal digital assistant, and a network-enabled phone.

Claim 43 (Currently Amended) A system comprising:

a target computing device;

a forensic device coupled to the target computing device via a customer network of the target computing device;

a client device; and

a user interface module to present a user interface for the forensic device that is remotely accessible by the client device, wherein the forensic device receives input via the user interface that identifies computer evidence to acquire from a target computing device and, in response, acquires the computer evidence from the target computing device without pre-loading acquisition software on the target computing device prior to acquiring the computer evidence, stores the computer evidence, and presents the computer evidence to the remote user for analysis via the user interface.

Claim 44 (Original) The system of claim 43, wherein the forensic device presents the user interface to the remote user to allow the remote user to view and analyze the data on-line.

Claim 45 (Original) The system of claim 43, wherein the forensic device acquires additional computer evidence from the target computing device while the remote user views and analyzes the previously acquired computer evidence.

Claim 46 (Original) The system of claim 43, wherein the forensic device acquires the computer evidence from the target computing device while the target computing device is active.

Claim 47 (Original) The system of claim 43, wherein the forensic device acquires state information from the target computing device.

Claim 48 (Cancelled)

Claim 49 (Previously Presented) The system of claim 43, wherein the forensic device receives input from the remote user that identifies at least one acquisition operation to perform, automatically selects at least one of a plurality of access methods via which to perform the acquisition operation based on the target computing device and type of computer evidence to acquire, and communicates commands associated with the acquisition operation to the target computing device to acquire corresponding computer evidence via the selected acquisition methods.

Claim 50 (Original) The system of claim 49, wherein the access methods include at least one of Windows Management Instrumentation (WMI), Server Message Block (SMB), Secure Shell (SSH), Remote Shell (RSH), Network File System (NFS), Apple Filing Protocol (AFP), File Transfer Protocol (FTP), and Hypertext Transfer Protocol (HTTP).

Claim 51 (Original) The system of claim 43, wherein the remote user identifies a plurality of acquisition operations to perform and the forensic device performs the acquisition operations in an order that reduces the impact on other data stored on the target computing device.

Claim 52 (Original) The system of claim 51, wherein the forensic device performs the acquisition operations to acquire at least one of a log file and communication statistics prior to any other acquisition operations.

Claim 53 (Original) The system of claim 52, wherein the forensic device performs an acquisition operation to acquire general system information from the target computing device after performing the acquisition operations to acquire the at least one of the log file and communication statistics prior to any other acquisition operations.

Claim 54 (Original) The system of claim 52, wherein the log file comprises one of a system event log, an application event log, a security event log, web server log file, Unix SYSLOG file, a mail log file, an accounting log file, and a router flow log file.

Claim 55 (Original) The system of claim 52, wherein the communications statistics comprises one of Ethernet statistics and network protocol statistics.

Claim 56 (Original) The system of claim 43, wherein the forensic device receives authentication information from the user to verify the identity of the user, the authentication information comprising one of a digital certificate or a username and password.

Claim 57 (Original) The system of claim 43, wherein the forensic device receives case information and target device information from a user to define a new inquiry, creates a new inquiry based on the received information, and associates the new inquiry with a case.

Claim 58 (Original) The system of claim 57, wherein the case information comprises at least one of a case number, case name, principle investigator, location to store the collected data, and a time zone for date/time reporting.

Claim 59 (Original) The system of claim 57, wherein the target computing device information includes at least one of a target computing device host name, IP address, operating system, access methods and password.

Claim 60 (Original) The system of claim 53, wherein the forensic device stores a copy of the computer evidence originally acquired from the target computing device, normalizes the acquired computer evidence to a common format, stores the normalized computer evidence, performs a cryptographic hash on the computer evidence, and stores the resulting hash value.

Claim 61 (Original) The system of claim 43, wherein the forensic device maintains an audit log of transactions to track at least one of computer evidence downloaded from the target computing device, browsing of the computer evidence by the remote user, and analyses performed on the computer evidence, and wherein the audit log comprises a timestamp corresponding to each transaction, an investigator identifier corresponding to the investigator performing each transaction, and a description of each transaction.

Claim 62 (Original) The system of claim 53, wherein the computer evidence comprises at least one log file, and wherein the forensic device analyzes the log file to detect log file tampering and displays to the user the results of the analysis.

Claim 63 (Original) The system of claim 62, wherein the forensic device determines whether the entries in the log file are in ascending order.

Claim 64 (Original) The system of claim 62, wherein the forensic device computes time gaps between entries of the log file, identifies anomalous time gaps, and displays to the user the identified anomalous gaps.

Claim 65 (Original) The system of claim 62, wherein the forensic device computes time gaps between entries of the log file, generates a graphical representation of the time gaps, and displays the graphical representation to the user.

Claim 66 (Original) The system of claim 62, wherein the forensic device receives input identifying a period and an identifier associated with a periodic event, searches the log file for the periodic event identifier, computes the amount of time that elapsed between each of the periodic event identifiers, and compares the period of the event with the computed elapsed times to detect an absent periodic event, and alerts the user of the absent periodic event.

Claim 67 (Original) The system of claim 43, wherein the forensic device acquires an image of at least one of a disk attached to the target computing device and a memory of the target computing device and examines the acquired image to identify at least one of files, process or operating system data structures, boot information, deleted files or directories, and data hidden in unallocated space.

Claim 68 (Original) The system of claim 43, wherein the target computing device comprises one of a personal computer, a handheld computer, a laptop, a workstation, a router, a gateway device, a firewall device, a web server, a file server, a database server, a mail server, a print server, a network-enabled personal digital assistant, and a network-enabled phone.

Claim 69 (Previously Presented) The system of claim 43, wherein the forensic device is coupled to a same local subnet as the target computing device.

Claim 70 (Previously Presented) The system of claim 43, wherein the client device is coupled to the forensic device via one of a public network, a customer network of the target computing device, a phone line, a universal serial bus (USB), a wireless port, a serial port, a parallel port and an infrared link.

Claims 71 (Currently Amended) An interrogation method to remotely acquire computer forensic evidence comprising:

receiving input from a remote user that identifies computer evidence to be acquired from a target computing device;

determining an order in which to perform acquisition operations to acquire the computer evidence from the target computing device with reduced impact on other data stored on the target computing device, wherein acquisition operations to acquire at least one of an log file and communication statistics occur in the order prior to any other acquisition operations; and

communicating commands to initiate the acquisition operations on the target computing device in accordance with the determined order <u>without pre-loading acquisition software on the target computing device</u>.

Claim 72 (Original) The interrogation method of claim 71, wherein communicating commands associated with the acquisition operations to the target computing device comprises:

communicating commands associated with an acquisition operation to acquire at least one log file to the target computing device; and

communicating commands associated with an acquisition operation to acquire at least one set of communication statistics to the target computing device after the commands associated with the acquisition operation to acquire the log file.

Claim 73 (Original) The interrogation method of claim 72, further comprising communicating commands associated with an acquisition operation to acquire general system information to the target computing device after the commands associated with the acquisition operation to acquire the communication statistics.

Claim 74 (Original) The interrogation method of claim 71, wherein communicating commands associated with the acquisition operations to the target computing device comprises:

communicating commands associated with an acquisition operation to acquire communication statistics to the target computing device;

communicating commands associated with an acquisition operation to acquire log file to the target computing device after the commands associated with the acquisition operation to acquire the communication statistics.

Claim 75 (Original) The interrogation method of claim 74, further comprising communicating commands associated with an acquisition operation to acquire general system information to the target computing device after the commands associated with the acquisition operation to acquire the log file.

Claim 76 (Original) The interrogation method of claim 71, wherein the log comprises one of a system event log, an application event log, a security event log, web server log file, Unix SYSLOG file, a mail log file, an accounting log file, and a router flow log file.

Claim 77 (Original) The interrogation method of claim 71, wherein the communications statistics comprises one of Ethernet statistics and network protocol statistics.

Claim 78-109 (Cancelled)

Claim 110 (Currently Amended) A forensic analysis device that is adapted to operate as an intermediate device between a target computing device and a client device associated with a remote forensic investigator, wherein the analysis device comprises an acquisition module to acquire state information from the target computing device without pre-loading acquisition software on the target computing device prior to acquiring the computer evidence and store the state information on the forensic device while the target device remains active.

Claim 111 (Original) The forensic analysis device of claim 110, further comprising a user interface that allows the remote forensic investigator to view and analyze the previously acquired computer evidence on-line while the acquisition module acquires additional state information.

Claim 112 (Cancelled)

Claim 113 (Currently Amended) A computer-readable medium comprising instructions that cause a processor to:

receive, with a forensic device coupled to a target computing device via a customer network of the target computing device, input from a remote user of a client device that identifies computer evidence to acquire from the target computing device;

acquire the computer evidence from the target computing device with the forensic device without pre-loading acquisition software on the target computing device prior to acquiring the computer evidence;

store the computer evidence on the forensic device; and

present a user interface for the forensic device through which the remote user views and analyzes, with the client device, the computer evidence acquired from the target computing device.

Claim 114 (Original) The computer-readable medium of claim 113, wherein instructions to cause the processor to present the user interface for the forensic device include instruction to present the user interface for the forensic device through which the remote user views and analyzes the computer evidence acquired from the target computing device on-line.

Claim 115 (Original) The computer-readable medium of claim 113, further comprising instructions to cause the processor to acquire additional computer evidence while the remote user views and analyzes the previously acquired computer evidence.

Claim 116 (Original) The computer-readable medium of claim 113, wherein instructions to cause the processor to acquire the computer evidence from the target computing device includes instructions to cause the processor to acquire the computer evidence from the target computing device while the target computing device is active.

Claim 117 (Original) The computer-readable medium of claim 113, wherein instructions to cause the processor to acquire the computer evidence from the target computing device includes instructions to cause the processor to acquire state information from the target computing device.

Claim 118 (Cancelled)

Claim 119 (Original) The computer-readable medium of claim 113, wherein instructions to cause the processor to receive input from the remote user that identifies computer evidence to acquire comprises instructions to cause the processor to receive input from the remote user that identifies at least one acquisition operation to perform, and further comprising instructions to cause the processor to:

automatically select at least one of a plurality of access methods via which to perform the acquisition operation based on the target computing device and the type of computer evidence to acquire; and

issue commands associated with the acquisition operation to the target computing device via the selected acquisition methods to acquire the computer evidence.

Claim 120 (Original) The computer-readable medium of claim 119, wherein instructions to cause the processor to issue commands associated with the acquisition operations comprises instructions to cause the processor to issue commands associated with the acquisition operations in an order that reduces the impact on other data stored on the target computing device.

Claim 121 (Original) The computer-readable medium of claim 113, further comprising instructions to cause the processor to:

store a copy of the computer evidence originally acquired from the target computing device;

normalize the acquired computer evidence to a common format;

store the normalized computer evidence;

perform a cryptographic hash on the computer evidence; and

store the resulting hash value.

Claim 122 (Original) The computer-readable medium of claim 113, further comprising instructions to cause the processor to maintain an audit log of transactions performed by the forensic device.

Claim 123 (Previously Presented) The system of claim 43,

wherein the client device is positioned remote from both the forensic device and the target computing device, and

wherein the client device is coupled to the forensic device by at least one intermediate network.

Claim 124 (Cancelled).

Claim 125 (Previously Presented) The method of claim 1, wherein acquiring the computer evidence from the target computing device comprises acquiring the computer evidence from the target computing device without the target computing device being shut down.

Claim 126 (Previously Presented) The method of claim 1, further comprising obtaining an image of a memory of the target computing device.

Claim 127 (Previously Presented) The system of claim 43, wherein the forensic device acquires the computer evidence from the target computing device without the target computing device being shut down.

Claim 128 (Previously Presented) The system of claim 43, wherein the forensic device obtains an image of a memory of the target computing device.

Claim 129 (Previously Presented) The forensic analysis device of claim 110, wherein the acquisition module acquires the computer evidence from the target computing device without the target computing device being shut down.

Claim 130 (Previously Presented) The forensic analysis device of claim 110, wherein the acquisition module obtains an image of a memory of the target computing device.

Claim 131 (Previously Presented) The computer-readable medium of claim 113, wherein instructions to acquire the computer evidence from the target computing device comprise instructions to acquire the computer evidence from the target computing device without the target computing device being shut down.

Claim 132 (Previously Presented) The computer-readable medium of claim 113, further comprising instructions to obtain an image of a memory of the target computing device.